stations (not emulated extension sets) as well (to be explained later).

Alleged "substandard" service	Properly Used Extension	Improperly Used Extension
Effect on the emulated extension user	Same quality of service as a single mobile station	Generally, same quality of service as a single mobile station. Second call may be blocked if system uses simultaneous checks.
Effect on other customers and the cellular system	No effect on others and on network	No effect on others and on network

Alleged "substandard service"	1✓	2✓	3✓	4✓	5✓	6✓	7✓	8✓

(See pp. 14-15 for explanation of chart).

Allegation That Unique ESN Per Set is the "Key" to Effective Validation: McCaw[12] claims that the key to an "effective" validation process is the premise that each cellular unit has its own unique ESN, and implies that emulated extensions "undermine" that key. This is a technologically incorrect statement in terms of both the present MIN/ESN-based technology and also the longer term future technology. Therefore, all existing and proposed MIN/ESN-based anti-fraud methods use some other additional information (simultaneous or velocity checks, behavior comparisons, PINs, or radio signatures) for positive identification. In the longer term, as stated earlier in this document, all experts who have designed second generation cellular and PCS systems have recognized that MIN/ESN identification is a fatally flawed process and they do not use it.

In any case, there is ample contrary expert opinion and evidence that ESN is not the key to an effective validation process but rather is a fundamentally non-secure method which

[12] McCaw Comments Jan.'95, p.6.

must be supplemented in the short term and replaced in the long term by a trustworthy authentication process. Thus, the fundamental premise put forth by McCaw and other petitioners, is, in my view, not correct and not sustainable by the evidence of the many other anti-fraud methods now used and proposed both by McCaw and other carriers. It is also one cause of the incorrect emphasis in the proposed re-wording of Rule 22.919 which only addresses ESN-based fraud and ignores many other radio parameters which can be used for fraud.

Alleged "ESN is key to effective validation	1✓	2✓	3	4	5	6✓	7	8

(See pp. 14-15 for explanation of chart).

Allegation that Carriers Cannot Provide Service Without Specific Usage Information Per Unit or Account: McCaw[13] claims that without specific information to determine the usage associated with particular units and particular accounts, cellular licensees cannot economically provide their services. This has several possible underlying bases, all being without substantiation.

First, the most obvious implication is that emulated extension mobile stations somehow evade proper accounting and billing for air time used. As explained before regarding the "rip off" allegation, this is technologically incorrect.

A second possible implication is that system design and planning for adequate traffic capacity are somehow compromised by the presence of emulated extension mobile stations. This is also incorrect. The size and capacity of a cellular system is determined by the carrier's choice of the location, number and size of the cells, and the number of voice channels provisioned in each cell. There are physical upper limits on the number of voice channels in each cell. The entire process of design and continuing modification of the cell structure is driven by the

---

[13] McCaw Comments Jan.'95, p7-8.

current known and projected total traffic in the system and its geographic distribution at the peak busy hours of the day.

Experienced cellular system designers use a number of theoretical and empirical formulas, charts and tables which allow determination of the number of voice channels needed in a cell to support expected traffic. The traffic information used as the design "input" for these methods in a competent cellular system design is total per cell or per sector traffic data, taken from the actual operating statistics or "stats" of the system itself. Designers do not use the usage statistics of particular individual accounts or units for this purpose. The cellular central switch stores detailed operating statistics on overall traffic and its geographical distribution in each cell. The number of call attempts which are not fulfilled (so-called "blockage") due to temporary occupancy of all voice channels in the relevant cell(s) is recorded in minute detail, so the system designer can determine the cells or areas of the system where more capacity is needed. Competent extrapolations regarding future traffic growth are based on two general parameters: 1) the expected average traffic per customer, based on actual switch data and customer count; and 2) projections of future increases in number of customers based on sales plans of the carrier. Ultimately, of course, there is an interplay between sales planning and the installation and provisioning of additional capacity, and neither of these elements alone drives the other, but the two are planned in co-ordination.

The clear implication of the wording of the McCaw complaint is that the usage associated with particular units and particular accounts is necessary to this system design and planning process. From my experience I can definitively state that the usage associated with particular units and particular accounts is not used in the system design and planning process. Furthermore, such information, if it were desired, is already available per account (but not, of course, per mobile unit) for emulated extension customers, and is clearly stated as the total of the air time on each customer's ordinary bill. Therefore, I conclude

that the presence of emulated extensions, as well as all other types of customers who may have traffic usage which differs significantly from the average, is not an impediment to a competent system traffic design and growth plan.

Alleged "cannot provide service without particular account&unit (traffic) information"	1✓	2✓	3✓	4✓	5	6✓	7	8

(See pp. 14-15 for explanation of chart).

Allegations That C2+ Operational Methodology is Worthless and Absence of Fraud Experience from C2+ Customers is Meaningless: McCaw[14] claims that the precautions taken by C2+ regarding identification of the customer, ensuring that the customer is a valid cellular customer, prevention of assignment of the same ESN to two customers, and the like, are worthless. McCaw deprecates the absence of any prior fraud-related complaints regarding C2+ customers from carriers as meaningless and insignificant.

To consider the latter point first, based on my experience in the cellular industry, the absence of such complaints is, contrary to McCaw, an extremely significant point. If, as McCaw claims, the presence of C2+ customers increases system vulnerability to fraud, undermines the integrity of the system, prevents effective deployment of a number of anti-fraud tools, etc., then there must be some significant increase in the level of fraud in systems with a higher number of emulated extensions in use. By the same reasoning, there would be less fraud in areas where C2+ emulation service is not marketed or has a smaller number of customers. While I am aware of a number of interesting correlations between the amount of cellular fraud in various cities and to a number of other factors, such as general crime level, the level of various specific types of criminal activity, the number of non-citizens or undocumented immigrants (which relates to "call sale" fraud) and other factors, I am not

[14] McCaw Comments, Jan.'95. p.9.

aware of any known correlation between the presence of emulated extension mobile stations and the level of fraud.

Further, there is no technological reason or basis to substantiate a claim that there should be more fraud problems in one case than the other, or for emulated extension mobile stations than others. The absence of such correlation is therefore a significant indication that these alleged problems are not, in fact, present. The claim by McCaw that such correlation is not possible because the carrier does not know who are the individual C2+ customers is irrelevant if the overall system experience with fraud level is not significantly different for systems with high vs. low numbers of emulated extensions. In addition to overall system statistics, it is my understanding that such correlations could also be computed on a customer by customer basis, but that McCaw and other carriers who oppose use of emulated extensions have threatened to deny service to such customers once they are identified. The Commission can readily settle this issue definitively by appointing a third disinterested party, similar to the role of a master appointed by a judge in a civil court, to receive the necessary data in confidence from both C2+ and the carriers in various cities regarding the number of C2+ customers and the incidence of detected fraud. A master competent in statistics and correlation and regression analysis can readily analyze such data and determine the genuine correlations, if they are present, and distinguish them from well known statistical red herrings such as city size, level of anti-fraud detection activity, and other factors which would produce false correlations.

To return to the first point, subscription fraud (customers obtaining unpaid cellular service via fraudulent proof of identity) is known to be a substantial problem for many cellular carriers. McCaw[15] specifically mentions subscription fraud and denigrates the background checking done by C2+ in this regard. However, both carriers (and their sales and marketing agents) and

---

[15] McCaw Comments Jan.'95 p.9.

C2+ have access to the same credit reporting information sources, and there is no reason presented by McCaw that one investigation is more complete and reliable than the other. There is no information presented to show that C2+ or its agents suffer from subscription fraud. In fact, the C2+ statement that its customers have not reported any increased fraud activity and no cancellations of service due to a simultaneous or velocity check connected with their use of C2+ emulated extensions, which is not disputed by McCaw (although its significance is disputed by McCaw as noted in the previous paragraph) indicates that C2+ experience is equal to or better than the subscription fraud experience of ordinary mobile sets. There is no information given to indicate that C2+ has a higher level of subscription fraud than a carrier has with ordinary customers when C2+ is not involved.

C2+ states that they determine from picture identification that the customer is the person named on the cellular carrier bill[16]. In my experience, the same method is used by cellular carriers and their sales agents. McCaw complains that C2+ has no way of knowing whether the customer is in good standing with the cellular carrier. Based on my experience, there are two important responses to this: 1) In some cases, the emulation supplier is also a resale agent of the carrier, and does indeed know this information; and 2) Should the customer prove to be a "deadbeat," the carrier, by consequently denying service to the customer's MIN/ESN, would immediately and without any additional action, deny service to all the emulated extension mobile stations of that customer. In other words, the level of protection against bad credit risks is the same regardless of the number of emulated extensions possessed by the customer. McCaw's characterization and ridicule of these precautions is not justified since the precautions appear to be just as complete, and, in some cases even more complete than the investigative steps taken by many cellular carriers and their sales agents, in my experience.

---

[16] C2+ Reconsideration Dec.'95, p.8-11 and Appendix.

Alleged "worthless background check and meaningless absence of higher fraud from C2+ customers"	1✓	2✓	3✓	4✓	5✓	6✓	7✓	8

(See pp. 14-15 for explanation of chart).

Although not specifically mentioned by others, the innovative C2+ process of checking the ESN to be installed in a mobile station against a central data base via an encrypted data communication link before permitting installation is a technological feature to prevent fraud which is superior to that of most manufacturer's system known to me. Only Ericsson has indicated in a submission that they have a similar protective technology[17]. Most manufacturer's systems for installation of ESN do not have such a capability in the field, and are susceptible to operational abuse, misuse, or an attack which could in many ways circumvent their protection and allow them to be used for fraud, just as the Commission has stated earlier. Ultimately, most manufacturers' systems, although admirable in many ways, depend on employee's honesty. The C2+ system does not depend to the same extent on human honesty, but uses technology to prevent the unauthorized use of its equipment. Therefore, in certain ways, the C2+ system is more secure and more realistically designed for field use, in my technological opinion.

Allegation that Emulated Extensions Interfere with Technological Registration: McCaw[18] claims that a mobile station is continually registering on the system, which they claim is necessary to provide service to the station and for billing.

---

[17] Ericsson, Reply, Nov.'92, p.4. I have also been told that JRC (formerly Novatel) has a similar technology. These systems use the "erase before write" operational order to prevent leaving a valid ESN in the set if the user should attempt to switch mobile sets during the process. However, neither of these systems requires an encrypted communication to a central data base to prevent multiple ESNs in different field locations. Either of these manufacturer's systems used illicitly in conjunction with an initial unauthorized ESN duplication, could be used unknowingly to proliferate multiple copies of the same ESN

[18] McCaw Comments Jan.'95, p.12.

They claim that this registration imposes system costs, even when the subscriber is not using the phone to converse, and that there is a higher consequent cost for emulated extension mobile stations than ordinary mobile stations.

There is one correct statement in all of this. A mobile station does indeed register (identify itself to the base radio) even when there is no conversation[19], when so commanded by the base station. However, all of the other statements and conclusions in this section of the McCaw submission are incorrect, partially incorrect, or are based on outdated information.

Because of the relation of the underlying statements (one correct and others incorrect) and the incorrect conclusions drawn by McCaw, a meaningful response requires a brief explanation of the registration process. A cellular network can cause a mobile station to transmit a short identifying message on the control channel in a number of different ways for different purposes. Mobile stations built under several previous revisions of the TIA technical standards behave somewhat differently in detail, so for brevity I will describe the registration process followed by the vast majority of mobile stations now in use.

Mobile stations are capable of transmitting two primary types of registration messages (home v. roaming), and some others which will not be described here. Although some cellular systems never use registration for home customers at all, the base system generally transmits a message periodically which contains several status bits to indicate whether local and/or roaming mobile stations should register with the base station. The most important type, which is almost universally used for roaming mobile sets, occurs one time only, when a mobile station first enters in a system which requires registration (or when the

---

[19] This registration message, and other related identification messages which occur even when there is no conversation, is also the basis for criminals to obtain the MIN/ESN values from ordinary mobile stations in mass quantities by use of a false base station such as a so-called "NAM Reader" equipped with an antenna and located at a place with a large number of cellular customers, such as a busy road.

subscriber first turns on mobile power). The second type of registration is called autonomous registration. If so commanded by the base station mobile stations may send registration messages at periodic intervals. It is significant to note that there is a very important third type of registration which should have been in the cellular system design, namely a message to indicate that the mobile station is leaving the system (due to physically leaving an outer cell boundary or because the customer turns off the power). Unfortunately, the vast majority of cellular mobile stations do not do this[20], and the absence of this third type of registration is one of the reasons which cause practical real cellular systems to operate in a manner quite different than alleged by McCaw. The differences between what McCaw alleges and the operation of real systems are manifested in several ways.

The original intended system design purpose for autonomous registration was to locate the mobile station so that paging messages (which are the first step in the setup of a so-called mobile-terminated or mobile-answered call) could be issued only in the cell(s) where the mobile station is most likely located. Many cellular systems have control software (with names like "zone paging" or "dynamic paging") which is written for this purpose. However, in most real practical cellular systems today paging is ultimately transmitted in all cells in the system, regardless of any registration information.

The basic reason for this lack of reliance on registration for giving service to the mobile stations is the disparity between the number of messages per second which can be handled effectively by the forward control channel (base to mobile) and the reverse control channel (mobile to base). The former channel can handle just over 19 messages per second, while the latter can only handle 2 or 3 messages per second. Carriers soon discovered in the early 1980s that this concept of localization via frequent

---

[20] The new IS-54 standard calls for such a capability, but less than 4% of current mobile stations in the field have this capability.

autonomous registration messages was not productive, and actually interfered with the ability of mobile stations to begin calls (when they responding to a page or send a mobile-originated call setup message on the reverse control) channel by clogging the reverse control channel with autonomous registration messages. Keep in mind that this problem was discovered in the early 1980s, historically well before the first instance of an emulated extension mobile station, so there is no relationship between the problem of excessive autonomous registration messages and emulated extensions The carriers then found empirically that they were usually not affected adversely by paging in all the cells in the system due to the relatively high capacity of the forward control channel.

In short:

1. Registration is not required in order to give cellular service for mobile-originated calls in either home or roaming service. Registration is not necessary for the billing process either, since the mobile identifies itself at the beginning of each call.

2. Autonomous registration, when used at all, is often set by the system operator at such a low rate[21] that it is not useful for localizing paging or any other service related aspect of system operation. This is due to the fact that an autonomous registration rate frequent enough to be useful for localizing paging would (in most systems) interfere with the call setup process by clogging the reverse control channel with autonomous registration messages. Furthermore, the base system is not aware, in general, if a particular mobile station leaves the system, except for the specific case in which the mobile immediately enters another system which is linked to the home system by data communications. Some customers may turn off the mobile power (many customers do this in order to avoid being

[21] Typically in the range of one autonomous registration during a time interval of from 20 to 90 minutes. During this interval, a vehicle moving at 50 mi /h (80 km/h) can move 16 mi. (26km) to 72 mi. (120 km), a distance much larger than a cell, and even larger than some cities.

cloned by criminal "MIN/ESN snatchers" who lurk by busy roads with false base system transmitters used for this purpose) when they are not talking, and the system will still page them despite this. Some carriers use the zone paging software during non-busy hours only, or as a preliminary step before using system-wide paging. However, the almost universal practice in all cellular systems is to ultimately page throughout all cells in the system, regardless of any autonomous registration messages which may be available, and particularly for a busy system, during the busy hour of the day for almost all systems, or when there is no response to zone paging first. In that sense, registration is not necessary in order to give service in the form of mobile-answered calls either.

3. The only case in which registration is necessary as a pre-requisite to giving service is, in general, a one-time initial registration for mobile-answered calls in a visited system (roaming service[22]), and in some cases, an initial one-time registration in the home system as well. Following that, the system may, in many cases, either not use continuing autonomous registrations or use a very low rate of autonomous registrations.

4. Because there is an implication, although not a clear description, in the McCaw allegation that emulated extension mobile stations somehow use more system resources due to registration, it is necessary to reply with the following important points:

a. For a properly used set of multiple emulated extension mobile stations (that is with only one powered up at a time) the amount and nature of registration messages (initial and periodic autonomous registrations) is precisely

---

[22] And even this is not always required. Many customers who divide their time between several cities on a continuing basis subscribe to multi-city paging service and have a multiple NAM capability in their mobile station (one ESN value with multiple MIN values, each MIN being "local" to one of the cities). The purpose of such a method is to pay only local air time charges in each city, rather than the higher roaming air time charges in all but one.

the same as a single ordinary mobile station, no more and no less.

b. For an improperly used set of multiple emulated extension mobile stations, with more than one used at a time, there would be more registration messages than for a single ordinary mobile station. However, the negative impact of this would fall only on the customer who used these stations improperly, and not on the system as a whole. If the simultaneous operation caused a simultaneous or velocity check (explained later), this customer and only this customer would consequently likely be denied service. In a system which uses autonomous registration, the overall rate of registration messages is controllable by carrier-set parameters broadcast by the base system. There may be a hidden implication in the McCaw allegations that there is some system control channel registration traffic impact of this nature. However, a competent carrier will adjust the rate of autonomous registration messages in the system so that it is below the threshold of interference with call-related reverse control channel messages, and this adjustment is made without regard to the number of messages from any particular MIN/ESN. In short, there is no system impact in a properly adjusted system.

Alleged Registration problems	Properly Used Extension	Improperly Used Extension
Effect on the emulated extension user	Same quality of service as a single mobile station	Same quality of service as a single mobile station. Multiple improperly operated sets can produce simultaneous or velocity checks.
Effect on other customers and the cellular system	No effect on others and on network	No effect on others and on network

The vagueness of the allegation was such that it did not specifically mention this, but to respond more completely, there is an improved method of registration for IS-54 mobile stations

only, called Location Area (LA) registration, which does not use periodic autonomous registration messages. In this new system, each cell can be set up to broadcast an LA code number, and in general a number of contiguous cells would use the same LA code. When an IS-54 mobile station crossed from one LA code into another, it would then register. This new registration algorithm allows the operator to determine the location of the mobile station more accurately and in a more timely way, without the problem of a traffic jam on the reverse control channel. In such a system, paging restricted to only the cells in one location area would be a practical possibility, in distinction to the present situation.

This does not change the previous conclusions, namely no harm or burden on network resources for a properly operated emulated extension. Again, the only potential issue is not one of network resources, but is the same issue of possible simultaneous or velocity check, with a consequent possible cutoff of service to the improper emulated extension customer. In neither case is there any actual or potential harm to the network nor to other customers.

Alleged negative interaction with registration	1✓	2✓	3✓	4✓	5✓	6✓	7	8✓

(See pp. 14-15 for explanation of chart).

Claims of Impediment of Anti-Fraud Technology: McCaw[23] claims intolerable risk to the cellular industry's fraud prevention programs. This same argument is stated in different words in their claim that C2+ technology "undermines" efforts to detect multiple registration of the same ESN/MIN combination in different parts of the cellular network[24]. McCaw also claims that the emulated extension technology itself creates very serious opportunities for fraudulent use and prevents effective deployment of a variety of anti-fraud tools. McCaw also claims

---

[23] McCaw Comment Jan.'95, p.5.

[24] McCaw Comment Jan.'95, p.7.

that cellular network cannot support the C2+ technology without increasing the system's own fraud vulnerability. Since no specifics or substantiating information is given except for a single reference to RF signature technology, it is necessary to respond by considering the four most used types of technological anti-fraud methods which interact with the mobile stations.

The first type is a "subscriber behavior" data base which flags a call which does not agree with the subscriber's customary calling habits. For example, should a customer who normally makes only short calls, or only local calls, or only domestic long distance calls, or only long distance calls to one state, make a call which differs from any of these norms, that call is flagged and can be automatically disconnected, or intercepted, or it can merely be brought to the attention of a fraud control staff member for further investigation, all according to the procedures of the particular carrier. As one would expect, there are numerous "false alarms" with such a system, because most customers occasionally make a call which is not consonant with their customary habits.

Clearly, when multiple emulated extension mobile stations are used by the same customer(s) who were the source of the "customary habit" data file, they will continue to have the same habit(s) regardless of which mobile station or how many mobile stations they use. There is clearly no different result with regard to this type of fraud control for emulated extensions versus one mobile station. If a fraudulent "clone" mobile station makes a call which is different from the customary habits of the customer, detection of this is clearly unrelated to the presence or absence of emulated extension mobile stations. This method used <u>by itself</u> does not detect simultaneous use of two mobile stations with the same MIN/ESN, although other anti-fraud systems used by the carrier may do so. Therefore, there is no system effect, from this method <u>alone</u>, even for improper simultaneous use of two emulated extension mobile stations. McCaw's argument is self contradictory in that it states that the emulated extension is indistinguishable to the network, yet it

creates a risk to fraud detection. If it actually created a risk to fraud detection, this would be a distinguishable network difference. I conclude that this method is not at risk from emulated extension mobile stations.

Behavioral pattern interaction	1✓	2✓	3	4	5	6✓	7	8

(See pp. 14-15 for explanation of chart).

Behavioral tests	Properly Used Extension	Improperly Used Extension
Effect on the emulated extension user	no different from single station set	no different indication than a single station set
Effect on other customers and the cellular system	no effect on system or others	no effect on system or others

The second distinct anti-fraud method is the detection of simultaneous calls by two stations with the same MIN/ESN. Several available software systems will flag simultaneous calls by multiple mobile stations having the same MIN/ESN identification in real time, so they can be dealt with according to the procedures of the carrier. We will discuss this for analysis together with the closely related "velocity" test or "time and place" test. A velocity test flags two non-simultaneous calls which are closer in time than the known distance between two cells and the known maximum velocity of the mobile station would physically allow. For example, if the closest parts of two particular cells are separated by 10 miles, and the maximum known velocity of the mobile station in that area is 60 mi./h (or 1 mi /min.), then a call which ends in one of these cells should not be followed by another call which begins in the second cell within the immediately succeeding 10 minute interval. (Registration, discussed earlier, may also be optionally used as an event signaling the presence of the mobile station in a particular cell. False control channel signals due to a radio sneak path -- described previously -- in a system with improper radio coverage can also can produce false alarms for

simultaneous activity from a single ordinary mobile set.) These tests may be used both within one cellular system, and, via data communication links, between different cellular systems as described in TIA standard IS-41, which can optionally notify the "home" cellular system of the time of a registration message and the start and end time of individual calls made or received by one of its customers who is "roaming" in the service area of a visited cellular system. If the system software flags a call due to one of these tests, the flagged MIN/ESN is handled according to the policy of the home carrier. Many carriers deny service on all succeeding call attempts by mobile stations with that particular MIN/ESN, and assign an investigator to follow up with the customer of record.

If multiple emulated extensions are used properly, and never have power on simultaneously, there will be precisely the same indication with respect to simultaneous calls as for a single mobile station, with no false simultaneous indications. If multiple emulated extension mobile stations are operated by only one customer, that customer can physically transport himself or herself only as fast as indicated by a properly configured velocity test, and again there will be no false alarms. Only in the case of multiple people, such as husband and wife for example, operating two emulated extension mobile stations non-simultaneously but within a time interval flagged by the velocity test, is there a possible false alarm. McCaw[25] complains that simultaneous and velocity checks are a particular problem for emulated extension customers. In contrast, C2+ indicates that none of their customers have ever reported having service discontinued because of a simultaneous or velocity check, although McCaw disputes the significance of this report as discussed in the previous section regarding McCaw's allegations that C2+ procedures to prevent fraud are "worthless." Regardless of whether this is a serious or a negligible problem in magnitude, there is a simple solution to this for emulated

---

[25] McCaw Comment, Jan.'95 p.10.

extension customers, of course. The carrier can arrange with the customer who is known to have emulated extensions that the carrier will ignore or use shorter time interval parameters for velocity checks for that customer's MIN/ESN, but will treat any truly simultaneous use as a valid alarm and act according to the carrier's normal procedures for a simultaneous check. By doing this, the customer is abandoning a certain very slightly higher level of fraud protection from velocity tests, but has the greater convenience and lower cost of emulated extension service for various members of the family, like a home landline telephone extension. This is a technologically sound and reasonable approach, in my opinion. It should be clear without further elaboration that there is no negative effect on the network or other customers.

In my conclusion I want to draw an important logical distinction: There is no impediment or risk to technological simultaneous or velocity test <u>detection</u> in the case of proper or improper extension use. The issue is what the carrier then does according to their business policies following this. We again return to the contentious issue of information equitably shared between the carrier and the emulator or customers with emulated extension mobile stations. It is my understanding that the petitioning carriers do not undertake such suggested treatment of apparent velocity test checks, and that a standoff exists between these carriers and emulation suppliers such as C2+, in which the carriers threaten, on the contrary, to cut off service to all emulated extension customers[26].

Simultaneous & velocity check	1✓	2✓	3✓	4✓	5✓	6	7✓	8

(See pp. 14-15 for explanation of chart).

[26] C2+ Reconsideration, Dec.'95. p.12-13.

Simultaneous & velocity tests	Properly Used Extension	Improperly Used Extension
Effect on the emulated extension user	Simultaneous check, no different from single user station sets. Velocity check could be false-flagged in certain cases involving multiple users, but this can be avoided by carrier agreement to ignore or cross-check velocity tests for such customer, and customer agreement to the reduced level of fraud protection	Simultaneous use will be flagged, likely service will be suspended. In my opinion, the customer must bear responsibility for this.
Effect on other customers and the cellular network	no effect on network or others	no effect on network or others

A third method used by some carriers to prevent fraud requires each subscriber to manually enter a distinct supplementary identification number from the keypad of the mobile station at the beginning of the connection. This supplementary number is usually called a personal identification number (PIN). If the PIN does not agree with a data value corresponding to the MIN/ESN identification of the mobile station, the call is flagged and handled according to the policy of the carrier. The policy of most carriers who use the PIN method is to disconnect such a call. This method has both technological anti-fraud and customer inconvenience shortcomings of its own which will not be discussed here, but it is used by a number of carriers. There is no difference in system response to a single mobile station or the use of emulated extension mobile station(s) provided the customer enters the PIN. If this method is used without other anti-fraud methods (such as a simultaneous or velocity check), there is no difference in network response even if the emulated extension customer improperly uses two extension mobile stations simultaneously. There is no risk to fraud protection, since the use of a PIN provides no better and no worse protection to an emulated extension customer than to a single station customer. There is clearly no impact on other subscribers or the network.

PIN interaction	1✓	2✓	3	4	5	6	7	8

(See pp. 14-15 for explanation of chart).

Use of PIN	Properly Used Extension	Improperly Used Extension
Effect on the emulated extension user	No different from single station	No different from single station
Effect on other customers and the cellular network	no effect on network or others	no effect on network or others

A fourth method of fraud protection which is under evaluation by some carriers is the so-called "RF signature" (also called an "RF fingerprint") method. This method uses a special base receiver calibrated to detect normally insignificant unit-to-unit manufacturing variations in mobile stations, even if nominally the "same" (that is, of the same manufacture and type). These variations affect the waveform of the transmitted call setup or page response messages from the mobile station. This calibrated receiver is coupled to a computer data base which retains the values of the distinctive waveform measurements and cross-indexes them by MIN/ESN value. In a selection of nominally identical mobile stations, most of the stations will have measurable and distinctive small differences in their transmitted waveforms. Again, there are some potential anti-fraud shortcomings as well, but the RF signature method is under test for possible use by a number of carriers.

Let us assume the scenario where RF signature is widely used by carriers. Also, consider, for the benefit of the argument put forth by McCaw, that several emulated extension mobile stations will have identical MIN/ESN but distinctive RF signatures. An RF signature system will record the waveform data from the first mobile station encountered with a specific MIN/ESN in the system. If, later, a second mobile station appears having a distinctive RF signature but with the same MIN/ESN as the first station, the RF signature system will flag this as a non-identical mobile station, and treat it according to the policy established by the carrier. In most cases, the second mobile station will be

disconnected and denied further service. In general, the situation will be investigated with the customer of record to establish which "signature" matches which mobile station.

The most logical way to handle multiple emulated extension mobile stations for this scenario is for the carrier to store and save the waveform measurement data for both mobile stations, with both cross indexed to the same MIN/ESN, in the RF signature data base. This does require more memory space in the RF signature data base than a single mobile station, but it does not require more memory data space in the network control computer or other parts of the network, a point which is discussed later in this Report. For comparison, consider two other cases in which the carrier would also handle two mobile stations regarding RF signatures. One case is the ongoing repair of a mobile station which is temporarily or permanently replaced by another mobile station during the repair. This is the case for which the proposed wording under consideration would allow the manufacturer or the manufacturer's representative to change the ESN within the bounds of Rule 22.919. Another case is the MUSDN service offered by some carriers, in which two distinct mobile stations are used. The two cases are compared to the emulated extension case in the following table.

Feature\situation	Temporary mobile station to be replaced with permanent set	Properly (or improperly!) used Emulated Extension	MUSDN service
Memory storage in RF signature system	Equivalent to two stations (carrier will presumably eventually delete the entry for the temporary set according to a pre-arranged schedule allowing for normal repair time. Note additional co-ordination with repair shop.)	Equivalent to two stations	Equivalent to two stations
Memory storage in network control (explained later in this document)	Same as single station	Same as single station	Equivalent to two stations
Effect on fraud protection via RF signature	no risk on emulation customer, on network or others (multiple RF signatures stored)	no risk on emulation customer, on network or others (multiple RF signatures stored)	no risk on emulation customer, on network or others (multiple RF signatures stored)

McCaw[27] claims in particular that emulated extensions are incompatible with RF signature technology. Some particular comments are needed in connection with the RF signature method, because it is only under test and not yet in use, and the Commission is less likely to be familiar with it. The proponents of RF signature technology claim a very high degree of accuracy - so high, in fact, that the same mobile station can be repeatedly distinguished from other mobile stations to the necessary degree of precision. Thus, there would be no risk in having multiple mobile stations present and active in the network with the same MIN/ESN with regard to any potential inability to properly distinguish the two mobile stations via their unique RF signatures. The statement by McCaw that the RF signature anti-fraud system is at risk because of emulated extension mobile stations present in the network is contradictory to the claims of identification accuracy underlying their interest in the RF signature method in the first place. If the RF signature method is as accurate as necessary, then it clearly should accurately

[27] McCaw Comments, Jan.'95, p.7.

recognize a third (and presumably fraudulent) clone attempting to defraud either type of two-station customers, the emulated extension customer or the customer whose primary station is in for repair. Therefore, there appears to be no sustainable technological objection. The business issue apparently concerns whether or not the carrier is willing to enter two RF signature data base entries, and is one aspect of the larger issue mentioned earlier about the carrier equitably sharing information about emulation extension customers. There is no distinction to be drawn concerning the proper or improper (simultaneous) use of multiple emulated extension.

RF Signature	1✓	2✓	3	4	5	6✓	7✓	8

(See pp. 14-15 for explanation of chart).

To conclude on the allegation of harm to anti-fraud measures, there are no negative interactions with any of the four anti-fraud methods described above except for the improper (simultaneous) use of multiple emulated extension mobile stations which has the potential to trigger a false fraud alert in systems using simultaneous or velocity checks. In that particular case, the harm is confined to the customer who uses the emulated extensions improperly, namely service will be denied by most carriers. In no case is there any harm to the network or to other customers.

It is also significant to remark that the technology of changing the ESN can be used to restore a customer to fraud-free service after that customer has become a victim of cloning fraud. At the present time, the customer who is a victim must change his or her MIN (directory number) on all business cards, stationery, and in some cases the listing in the local telephone directory. By issuing a new ESN and retaining the same MIN, the customer and the carrier are spared this cost and inconvenience[28]. This has no relationship to the use of emulated extensions one way or the

[28] C2+ Reconsideration, Dec.'95, p.7 footnote.

other, but merely illustrates yet another legitimate benefit of ESN modification.

D. Conclusions and Recommendations: I conclude that there are no problems of network burden nor undesirable interaction with fraud-detection methods now in use, for the case of properly operated emulated extension mobile stations. The problems alleged in this connection in the documents which I have reviewed are, in fact, non-existent, and appear to be due to incorrect or outdated basic information regarding the design and current method of operation of real cellular systems. Even in the case of improperly operated emulated extension mobile stations, there is only one case in which there is a potential negative interaction, namely the case of simultaneous or velocity checks with improperly used emulated extension mobile stations, and in that case there is harm only to the improperly using customer. In no case is there any general network harm or harm to other customers resulting from the use of emulated extension mobile stations by bona fide cellular customers, unless the cellular system is improperly or incompetently operated by the carrier.

In my view, the use of emulated extensions provides a technologically superior method for providing extension service to those customers who desire extensions. The advantages of the emulated extension over services such as MUSDN relate to system simplicity, economy of resource use, and a superior level of service to the customer since all of the multiple emulated extension mobile stations are capable of roaming and temporarily selecting the competitive carrier, while all but one of the MUSDN-type extensions are not. Furthermore, the emulated extension does not require the carrier to expend any resources for either initial activation or on a continuing or recurring basis for additional emulated extensions.

There are two potential technological areas in which the carrier could store additional information regarding emulated extensions in use in the network which would remove the potential

problem noted above, thus removing even the potential problem for improper use.

a. Storage of information indicating multiple emulated extensions for a given MIN/ESN to adjust simultaneous checks and velocity checks. This information would consist of one bit in memory for that customer indicating the use of emulated extensions.

b. If RF signature equipment comes into use in the future, storage of the RF signature parameters for each emulated extension used by the customer. The parameter storage for each additional emulated extension mobile station would be equivalent to that an ordinary mobile station.

Should the carrier make the storage of this information an available option for customers, a reasonable charge should be levied on the relevant emulated extension customers only. If a customer does not make use of these capabilities when offered by the carrier, and consequently has service discontinued due to a velocity check or other cause arising from improper use, a reasonable charge for restoration of service should be levied. The customer should give informed consent to this. At the same time there should be corresponding safeguards to prevent abuse of the discretion of the carriers with regard to these activities.

With regard to the wording of the present Rule 22.919 adopted January 1995, and the changes proposed to allow only the manufacturer or its agent to change the ESN, my technological conclusions are:

1. Neither the present wording of Rule 22.919 nor the proposed modifications suggested by the TIA and CTIA will advance the cause of fraud prevention nor inhibit fraudulent cloning of cellular telephone sets, but instead will deny legitimate uses of modified ESN such as emulated extension service, and restoration of service to victims of fraud without change in directory number.

2. There is a single-minded emphasis on the ESN alone in these prior suggested wordings, although it is known to many experts in the industry that a number of other parameters of the

mobile station can be altered to contribute to fraud, and they are not addressed. This is likely to lead to continual repeated reconsideration of this and related sections again and again as each new type of fraud becomes more prevalent, rather than addressing all of them now with a properly worded rule. I will submit a separate proposal on my own behalf to address this point.

3. The prohibition against changing the ESN and the three specific methods in the present wording for software treatment of the ESN do not technologically prevent or even increase the difficulty of fraudulent "cloning" by criminals. Their only foreseeable effect on the industry is to prevent legal provision of emulated extension mobile stations, or replacement stations with the same MIN but new ESN for fraud victims.

Oath: I declare under penalty of perjury that the facts set forth in this report are true according to the best of my knowledge, information and belief.

Richard C. Levine

Richard C. Levine